UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/566,206	06/05/2006	Kezhi Qiao	00698000001	5525

22907 7590 10/25/2007

BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
10/25/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/566,206	QIAO ET AL.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 August 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 January 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *8/23/07*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The amendment of 23 August 2007 has been noted and made of record.

2. Claims 1-7 have been presented for examination.

Response to Arguments

3. Applicant's arguments with respect to claims 1-7 have been considered but are moot in view of the new grounds of rejection.

4. See further rejections set forth below.

Information Disclosure Statement

5. The information disclosure statement (IDS) submitted on 23 August 2007 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner has considered the information disclosure statement.

Claim Rejections - 35 USC § 103

6. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

7. Claims 1, 3, and 5-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication No. 2005/0220078 to Luken, hereinafter Luken, in view of RFC 3525: Gateway Control Protocol Version 1, hereinafter RFC 3525, and in further view of U.S. Patent No: 7,089,211 B1 to Trostle et al., hereinafter Trostle.

8. As per claim 1, Luken teaches a system comprising a media gateway (Figure 1 [blocks 26 and 40]) and a Media Gateway Controller (Figure 1 [blocks 36, 44]). Luken also discloses that the Media Gateway Controller can be used to verify digital signatures (paragraph 0064), which are based on keys.

9. Luken does not teach generating a session key based on the digital signature to be used to communicate between the two devices and renewing a session key when the previous session key has expired.

10. RFC 3525 teaches that the media gateway controller can provide media gateways with session keys (printed page 72 of 200, Section 10.3 Protection of Media Connections), similar to page 5 of the Applicant's disclosure.

11. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the media gateway controller to provide session keys to the media gateways, since RFC 3525 states at printed page 72 of 200 that the session keys can be used to encrypt the audio messages, thereby protecting against eavesdroppers.

12. Neither Luken nor RFC 3525 disclose updating the session key after it has expired.

13. Trostle teaches the updating of session keys in response to normal expiration or other causes (column 10, lines 50-52).

14. It would have been obvious to one of ordinary skill in the art at the time the invention was made to update the session key when it expired, since Trostle states at column 10 lines 45-50 that key updates are vital to maintain the secure nature of the communication.

15. Regarding claim 3, Luken teaches for each call, attaching a digital signature to each call message from said Media Gateway Controller to said Media Gateway by using said shared key (paragraph 0064);

validating said digital signature in said call message in said Media Gateway by using said shared key, and if it is valid, returning a response message attached with a digital signature using said shared key to said Media Gateway Controller (paragraph 0064); and

validating said digital signature in said response message in said Media Gateway Controller by using said shared key, if it is valid, setting up a call service (paragraph 0020, i.e. establishing a connection), otherwise denying the call (paragraph 022, i.e. rejection message).

16. With regards to claim 5, Luken teaches that the algorithm used to generate a shared key by said Media Gateway Controller and said Media Gateway is different from the algorithm used to generate a digital signature by said Media Gateway Controller and said Media Gateway (paragraph 0064, i.e. Algorithm field).

17. With regards to claim 6, Luken teaches that a field/packet of an expanded protocol is used to transmit said parameter for generating a shared key and said digital signature (paragraph 0064, i.e. key and digital signature).

18. Regarding claim 7, RFC 3525 discloses the use of session keys as discussed above. Session keys include a lifetime the key that is either time or the number of times said shared key can be used as noted by page 216 of Stallings.

19. Claims 2 and 4 rejected under 35 U.S.C. 103(a) as being unpatentable over Luken in view of RFC 3525 and Trostle as applied to claim 1 above, and further in view of **Cryptography and Network Security**, by William Stallings, hereinafter Stallings.

20. Regarding claims 2 and 4, Luken teaches generating a new shared key further comprises:

initiating a register signaling from said Media Gateway to said Media Gateway Controller to register, wherein said register signaling has a parameter for generating a shared key and a digital signature generated by said initial key (paragraph 0064).

21. RFC 3525 teaches generating a shared key (i.e. session key) as discussed above. Furthermore, since RFC 3525 discloses the use of session keys the lifetime of said shared key after said Media Gateway Controller has validated said Media Gateway with said initial key should be set as noted with respect to claim 7.

22. Neither Luken, RFC 3525, and Trostle teach initiating a modification command from said Media Gateway Controller to said Media Gateway, wherein said modification command has a parameter for generating the shared key, a digital signature generated by said initial key and a lifetime of a shared key; and generating the shared key and setting up the lifetime of said shared key after said Media Gateway has validated said Media Gateway Controller with said initial key.

23. It would have been obvious to one of ordinary skill in the art at the time the invention was made to generate a new shared key, since Stallings states at page 216 that the more frequently the session key are exchanged, the more secure they are, because the opponent has less ciphertext to work with for any given session key.

Conclusion

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

25. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

26. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131

Clf